Published in

LAW360

CPA CYBERSECURITY FRAMEWORK MAY BE VITAL TOOL

By Christian Leitner, Director IT/IS Assurance

General information technology threats targeting organizations across many different industries are emerging in an alarming rate. Business email compromise, ransomware and other malware attacks cost American businesses billions of dollars last year. Furthermore this is all aggregated by the trend of cloud computing applications, which also have been heavily adopted by many law firms.

For example, law firms have become a lucrative target for cybercriminals. Their systems usually contain personal information of clients and business partners.

The Panama Papers scandal in 2015 made this growing threat evident – 11.5 million documents containing sensitive client information and financial records were leaked from a Panama-based law firm. Leaking of information is a serious problem for any law firm and could be an existential threat. Brennan Torregrossa, vice president, associate counsel and head of the global external legal relations team at GlaxoSmithKline LLC, said: ”The trust between a law firm and a client is fundamental to a productive attorney-client relationship.

A vital way for law firms to gain client trust is to protect the confidential information provided to them by their clients from cyber threats.”

The American Bar Association recently published an article that talks about cybersecurity and law firms and how to address this business risk. The FBI and the SANS institute also have been working with law firms to address the raising cybersecurity risk for these entities.

Cybersecurity might be the biggest risk law firms face in 2017. One reason is that it is a self-governing profession. Regulations like the Health Insurance Portability and Accountability Act in the health care industry do not exist for law firms.

Nevertheless, sensitive and valuable information of clients and business partners are in the custody of these organizations. Law firms will need to invest a significant amount of time and money to maintain the trust of their clients and business partners. It will be the law firm’s obligation to convince them that their data is secure with them.

What does a law firm’s website say about its cybersecurity? Plain and outdated-looking websites can tell an attacker more than you think about your security practices. Websites like these are an indicator that a firm has not kept pace with technology and does not recognize its value, which makes them easy targets for a large variety of cyberattacks. This usually applies more to smaller law practices.

How to strengthen your firm’s cybersecurity:

- Protect client data by granting access on a need-to-know basis.
- Perform IT audits at least annually and re-evaluate your risk assessment periodically.
- Introduce employee awareness trainings. Your users are usually the weakest link within your security measures.
- Insist on rigorous compliance standards for hosted software.
- Hire outside experts to test and evaluate your security measures.

Cybersecurity is no longer a topic discussed during IT meetings and it has now become a business conversation. More and more board and audit committee members across the nation view cybersecurity and loss of company reputation as a major risk that will need to be paid more attention to in the future.

In order to do this, board members and owners should get involved and ask security professionals within their organizations the following questions:

- Do we have a wire policy that will protect us from business email compromise attacks?
- Are all our critical systems backed up on a regular basis to restore data potentially compromised by ransomware or malware?
- How do we select and evaluated cloud service providers? Are service organization control reports available?
- How would we respond to an incident or breach? Do we have an incident response plan?
- Is it documented? When was it last tested?
- Have we considered cyber liability insurance?

In May 2017, the American Institute of Certified Public Accountants released its long-awaited Cybersecurity Attestation Framework. Also known as service organization control (SOC) for cybersecurity, this framework builds on top of the long-established trust services principles (TSPs) reporting. TSPs are the underlying criteria for SOC reports, but were usually limited to one or more systems delivering services to an organization's customers. The newly released framework uses these TSPs, but applies them across an entire law firm instead of just a specific system or department. In what could be seen as "SOC reporting on steroids," the scope is much larger and covers all aspects of a firm's cybersecurity program. The purpose of such an attestation is to deliver an independent evaluation by a certified public accountant registered and in good standing with the AICPA. CPAs are in the unique position to perform these audits given the AICPA standards, which are available to the public and whose scope is the same for every firm. Many CPAs are currently promoting this as a separate service line to be performed annually or semiannually.

The application of the reports could make it a vital tool in the future regarding how to deal with cybersecurity questions related to your own law firm, your clients and other third parties identified during your risk assessment. The independence factor will move this approach above the existing self-monitoring and self-assessment reports given to stakeholders. For example, the law firm will get the report addressing the effectiveness of its cybersecurity program according to the TSPs and can then use it to show internal (e.g., partners and executive committees) or external (e.g., clients and outside counsel) stakeholders that their program can be relied upon.

While the AICPA framework is still in its adoption phase, it received a lot of positive feedback prior to its release in May from early adopters and professionals in the cybersecurity field. The general consensus is that the framework will open new ways for law firms across the U.S. to deal with cybersecurity questions and help evaluate internal and external cybersecurity risks from a business perspective.

Christian Leitner, Director IT/IS Assurance, is a certified information systems auditor at OUM & Co. LLP, a CPA firm with offices in San Francisco and San Diego. He has been leading Sarbanes-Oxley IT audits, SSAE16 SOC1/SOC2/SOC3 engagements and other IS compliance consulting projects since 2004.

San Francisco, CA
415.434.3744
Carlsbad, CA
800.208.3367
oumcpa.com

OUM &CO. LLP ACCOUNTANTS & BUSINESS ADVISORS